Clase de Seguridad

DC - FCEyN - UBA

05 de Noviembre de 2014

Menú del día

Definición

Seguridad en algún punto implica ausencia de **riesgo**. Esto puede depender de nociones abstractas y sociales como la **confianza**.

Problema

En las redes, y por sobre todo en la Internet, es muy complejo estar exento de posibles **vulnerabilidades**. Lo ideal es identificar los riesgos más peligroso respecto a la información que se desea resguardar y tomar las **medidas** pertinentes y factibles según la relación costo / beneficio.

¿Es seguro?


HACKED
©Beyond Security® All rights reserved
www.SecuriTeam.com
BY DALE BRADEN
I'M NOT USING THIS CIRCUIT UNTIL I KNOW FOR SURE THAT OUR CONVERSATION WILL OCCUR OVER A SECURE CONNECTION!

Principales aspectos que atañen a la seguridad

- Confidencialidad.
- Integridad.
- Disponibilidad.

Las leyes, coyuntura, individuos y organizaciones definen los diversos grados de **riesgo** que se puede **mitigar o soportar** respecto a estos conceptos bajo ciertos entornos.

Confidencialidad

Es el **ocultamiento o encubrimiento** de información y/o recursos. Los mecanismos de **control de acceso** son los encargados de preservar este rasgo de la información. Si son vulnerados o **comprometidos**, se pierde la propiedad y la confidencialidad es corrompida. A veces es tan o más importante proteger el mero conocimiento de la existencia de la información que el contenido de la misma.

Integridad

Es la prevención para que no sucedan **modificaciones impropias o sin autorización** en la información. Existe tanto la integridad de los **datos** como la integridad de **origen**. Mecanismos de autenticación y control de acceso sirven para atenuar el riesgo de comprometer este rasgo de la información. Suele ser más dificultosa de proveer que la confidencialidad.

Disponibilidad

Concierne la **posibilidad** de **utilizar** el recurso o la información necesaria. Se suelen utilizar mecanismos estadísticos sobre patrones de utilización de datos para asegurar la disponibilidad. Los famosos ataques de **denegación de servicio** apuntan a vulnerar este concepto.

Amenaza

Es una **potencial** violación de algún rasgo concerniente a la seguridad. No necesariamente tiene que realizarse. Las acciones que permiten que se concrete son denominadas **ataques**.

Políticas vs. Mecanismos

- Una política o norma de seguridad describe qué está permitido y qué no.
- Un mecanismo de seguridad es un método, herramienta o procedimiento que fuerza el cumplimiento de la política.

Resumiendo...

Dada una especifícación (formal o informal) de una política de seguridad describiendo qué es seguro o permisible y qué no, se deben implementar los mecanismos de seguridad adecuados para **prevenir** los posibles ataques, o en su defecto **detectarlos** y poder recuperarse de ellos. Es importante notar que a veces alcanza con simplemente **identificar** y actuar.

Definición

El estado de protección de un sistema es el **conjunto de valores** de los recursos que repercuten en la seguridad del sistema (memoria principal, secundaria, registros). La matriz de control de acceso es una herramienta que permite **describir** los estados de protección.

El modelo

Caracterizar los permisos de cada **sujeto** respecto a cada **entidad** del estado de protección. Un ejemplo de este modelo es la matriz de acceso de los sistemas Unix.

Ejemplo

Objetos: File 1, File2, Process 1, Process 2.
Sujetos: Process 1, Process 2.
Permisos: Leer, escribir, anexar, ejecutar, ser dueño de...

	File 1	File 2	Process 1	Process 2
Process 1	r,w,o	r	r,w,x,o	w
Process 2	a	r,o	r	r,w,x,o

Limitaciones

La matriz de control de acceso es el **modelo abstracto** principal para describir modelos de seguridad. Formalmente, es capaz de expresar **cualquier** política de seguridad, pero en la práctica no sirve porque no **escala**. Se usa solo en ciertos casos como el ejemplo anterior donde los objetos y sujetos no son demasiados y también para análisis teóricos.

Limitaciones teóricas

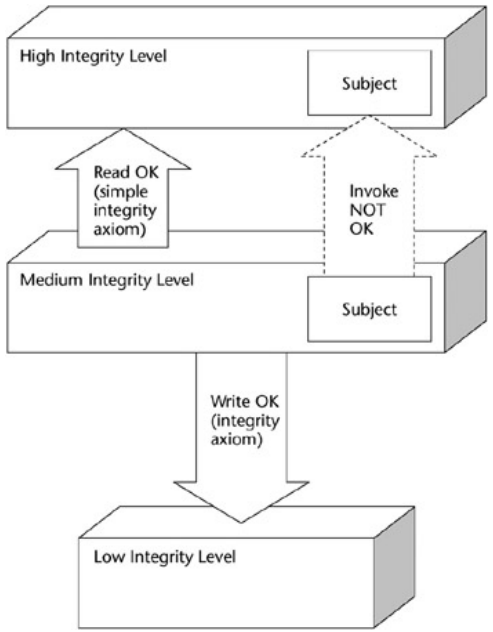
Sería interesante encontrar un modelo que defina el estado de la máquina y luego ejecutar algún **algoritmo**, que dado un estado **responda** si éste es seguro o no. Sin embargo, existe un **teorema** que postula que es **indecidible** dar a conocer si un estado de protección es seguro dado un permiso genérico.

Bell-LaPadula

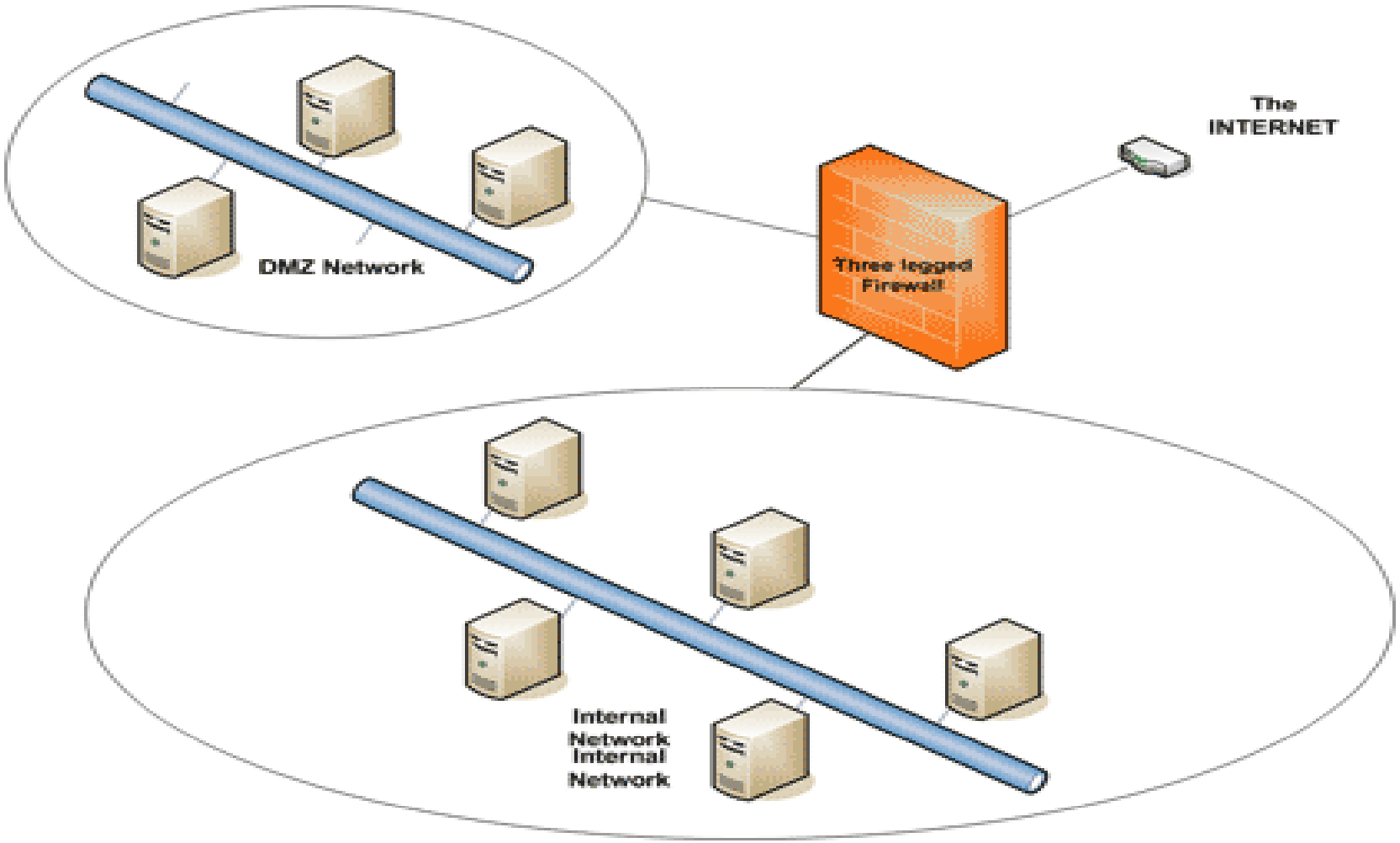
Orientado a proveer confidencialidad. La integridad es secundaria. Se definen niveles de seguridad para los objetos y sujetos. Ningún sujeto puede acceder a objetos que pertenzcan a niveles de seguridad más altos que el de si mismo.

Biba, Clark-Wilson

Orientado a proveer integridad. La confidencialidad es secundaria. Se definen niveles de seguridad para los objetos y sujetos. Ningún sujeto puede escribir a objetos que pertenzcan a niveles de seguridad más altos que el de si mismo y leer objetos de niveles inferiores.



Definición

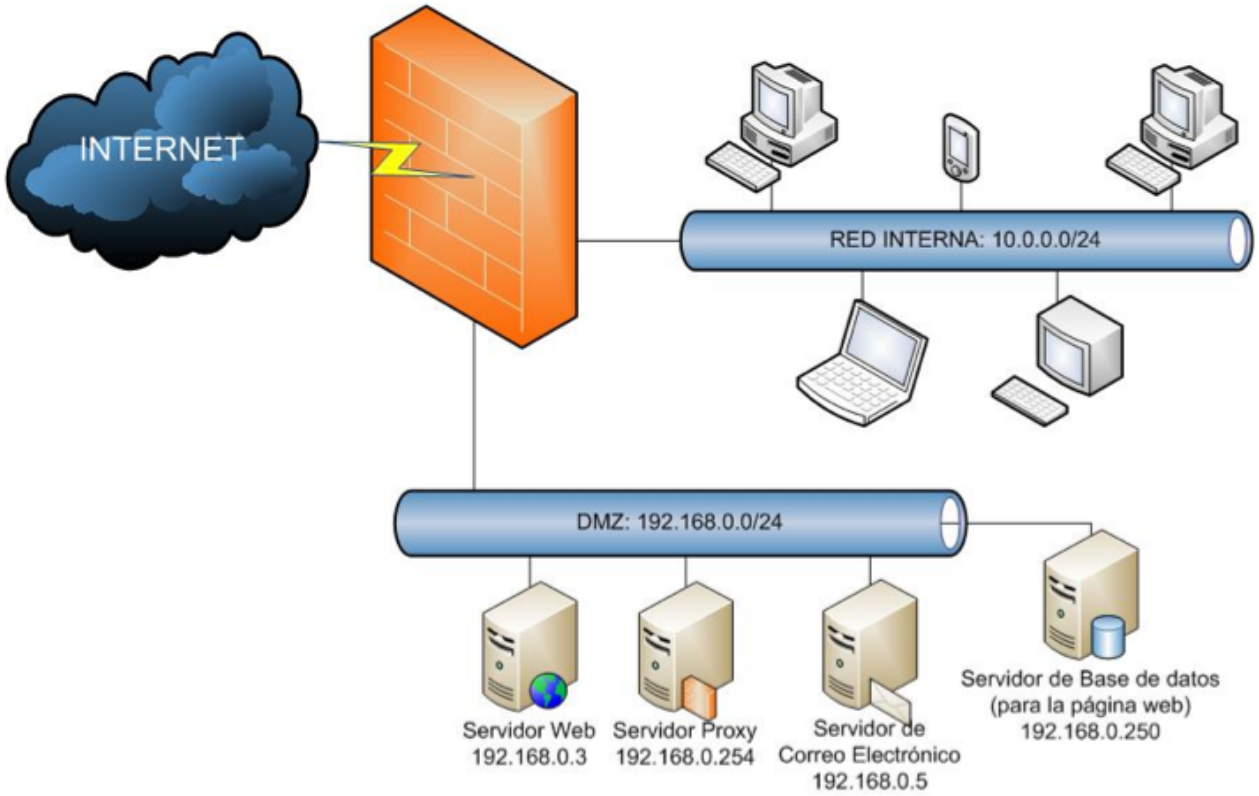

The
INTERNET
Three legged
Firewall
DMZ Network
Internal
Network
Internal
Network

Distintos tipos

- **Filtrado de paquetes**: Cada paquete es verificado individual y independientemente de los demas y permitido o denegado dependiendo de un conjunto de reglas estáticas.
- **Stateless**: Utiliza reglas sencillas sobre los mensajes entrantes / salientes del tipo:
  $< addr\_in, port\_in, addr\_out, port\_out, proto >$
- **Stateful**: Mantiene estado de conexiones entrantes o salientes y puede permitir o denegar teniendo en cuenta la sesion a la que pertenece.
- **Gateways de circuito**: Proxy no inteligente. Reenvía la conexión.
- **Gateways de aplicación**: Proxy inteligente. Entiende ciertos protocolos. Sirve para aplicar filtros de capa de aplicación.

Firewall

Definir reglas y políticas de seguridad a implementar en un firewall con estado bajo la siguiente organización. Explicitar asunciones:



Asunciones

Politica de filtrado por defecto: **DROP**.

- Servidor de mail usa POP3 e IMAP.
- Servidor web usa solo HTTP.
- El servidor web es autónomo, no necesita resolver nombres ni salir a inet.
- El servidor de bd solo se usa para los sitios web.

Reglas

DESDE□HACIA	INTERNET	DMZ	RED INTERNA
INTERNET		Servidor Web: HTTP Servidor Mail: SMTP	**DROP**
DMZ	Servidor Mail: DNS Servidor Mail: SMTP Servidor Proxy: DNS Servidor Proxy: HTTP Servidor Proxy: HTTPS		**DROP**
RED INTERNA	**DROP**	Servidor Web: HTTP Servidor Proxy: PROXY Servidor Mail: SMTP Servidor Mail: POP3 Servidor Mail: IMAP	

Definición

Un sistema criptográfico es una tupla (E,D,M,K,C) tal que:

- M es el conjunto de los **textos válidos**.
- K el conjunto de **claves**.
- C es el conjunto de los textos cifrados.
- E: M x K $\rightarrow$ C.
- D: C x K $\rightarrow$ M.

Objetivo

Mantener la información encriptada **secreta** siempre y cuando la clave se mantenga **escondida**. Si se conoce el algoritmo de encriptación mejor.

Taxonomía

- Criptografía Moderna
  - Cript. Simétrica (clave secreta)
    - Cifrado de Flujo
    - Cifrado en Bloque
  - Criptografía Asimétrica
    - MDC (sin clave)
    - MAC (con clave)
  - Funciones de Hashing

DES

- Orientado a **bits** y no a caracteres.
- Usa tanto transposición como sustitución.
- Trabaja en **bloques** de a 64 bits.
- Cada bloque ejecuta 16 iteraciones con **distintas** claves.
- Fue mainstream durante muchos años. Con el tiempo fue quedando obsoleto el largo de la clave y los ataques por fuerza bruta comenzaron a ser computacionalmente rápidos. También se le encontraron vulnerabilidades para algunas claves específicas.
- 3DES.
- AES es recomendado hoy en día. Claves más largas, es más rápido y resuelve las vulnerabilidades encontrardas en DES.

Conceptos

Diferentes claves para cifrar y descifrar. A diferencia de los métodos clásicos no se debe compartir una clave secreta. Una de las claves es **pública** y la otra (**secreta**) es privada.

Se deben cumplir tres propiedades

- Debe ser fácil cifrar o descifrar dada la clave adecuada.
- Debe ser inviable computacionalmente derivar la clave privada a partir de la pública.
- Debe ser inviable computacionalmente derivar la clave privada a partir de un texto descifrado.

RSA

Los conceptos teóricos que sustentan este algoritmo son ciertas propiedades **matemáticas** respecto a los **números primos** (factorizar números grandes es costoso), módulos y exponenciación. Un algoritmo puede encontrar un par de claves, que debido a estas propiedades **no son derivables** una de la otra, pero tienen la propiedad de ser la **inversa**.

Diversos usos...

- No repudio.
- Integridad.
- Confidencialidad.

Message digest

Consiste en adosarle al mensaje a enviar un checksum que luego puede ser recomputado y constatado para verificar la integridad (igual que en ip). Para proveer seguridad se usan funciones de hash con clave o se cifran los hash sin clave.

Funciones de hash fuertes (buenas o de ida) $h : A \rightarrow B$

- Dado $x \in A, h(x)$ es fácil de computar.
- $\forall y \in B$ es (comp) inviable encontrar $x \in A$ tq $h(x) = y$.
- es (comp) inviable encontrar $x, \hat{x} \in A$ tq $x <> \hat{x}$ y $h(x) = h(\hat{x})$.

Mejores algoritmos conocidos actualmente

- MD2
- MD4
- MD5
- SHA-1
- HAVAL

HMAC

Consiste en hashear el mensaje mezclado con la clave de una manera standard. Sirve para proveer **integridad**. Está demostrado que la seguridad de HMAC depende de la función de hash que se utilice.

Tipos de claves

- Claves de intercambio: Asociadas a un ente (máquina / persona).
- Claves de sesión: Asociadas a una comunicación.

Se usan claves de sesión nuevas por cada comunicación permitiendo disminuir las posibilidades de ataques estadísticos.

Generar clave de sesión

Confiar en un tercero (Cathy)

1. Alice $\rightarrow$ Cathy: $\{$ Request de clave de Sesion con Bob $\}K_{Alice}$
2. Cathy $\rightarrow$ Alice: $\{K_{ses}\}K_{Alice} \mid\mid \{K_{ses}\}K_{Bob}$
3. Alice $\rightarrow$ Bob: $\{ K_{ses} \}K_{Bob}$

Kerberos

Es un servicio que provee claves de sesión basado en el algoritmo anterior. En la realidad es bastante más complejo ya que evita el **man-in-the-middle** o otras posibles vulnerabilidades.

Usando criptografía de clave pública

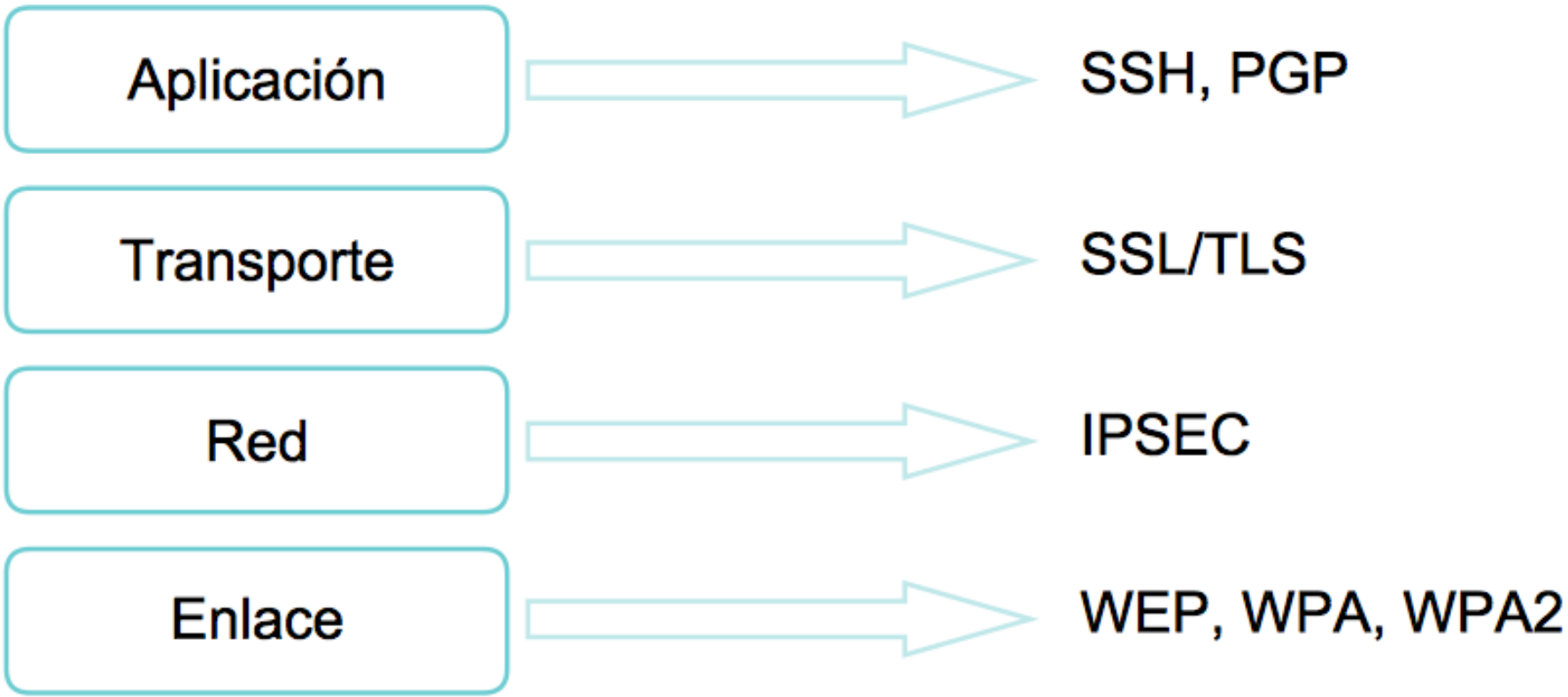
Alice $\rightarrow$ Bob: Alice, $\{ \{ K_{ses} \} D_{Alice} \} E_{Bob}$

Desafíos

La cuestión más importante es la validación y manejo de las claves públicas y privadas.

Aparecen los **certificados** que básicamente son relaciones entre claves públicas y cierta entidad. Para darle validez a estos certificados se confía en **autoridades certificantes** o **cadenas de confianza**.
X.509v3 es el estándar de que define los formatos de certificados.

¿En qué nivel?


Aplicación
SSH, PGP
Transporte
SSL/TLS
Red
IPSEC
Enlace
WEP, WPA, WPA2

TLS

- Versión actualizada de SSL (Secure Sockets Layer).
  - La última versión de SSL (Netscape) fue 3.0
  - TLS se identifica como SSL v 3.1.
  - Similar, pero no compatible directamente.
  - Especificado en RFC 2246 (1999). Extendido posteriormente en RFC 3546 (2003).
- Protege una sesión entre cliente y servidor. El caso más conocido es HTTP (navegador y web server).
- Requiere protocolo de transporte confiable, por ejemplo TCP.

Servicios

- Autenticación.
  - Del servidor frente el cliente
  - Opcionalmente, del cliente frente al servidor.
  - Mediante **certificados** de clave pública.
- Integridad.
  - Mediante **MAC** y números de seq.
- Confidencialidad.
  - Opcional.
  - Mediante **cifrado** con algoritmo simétrico.

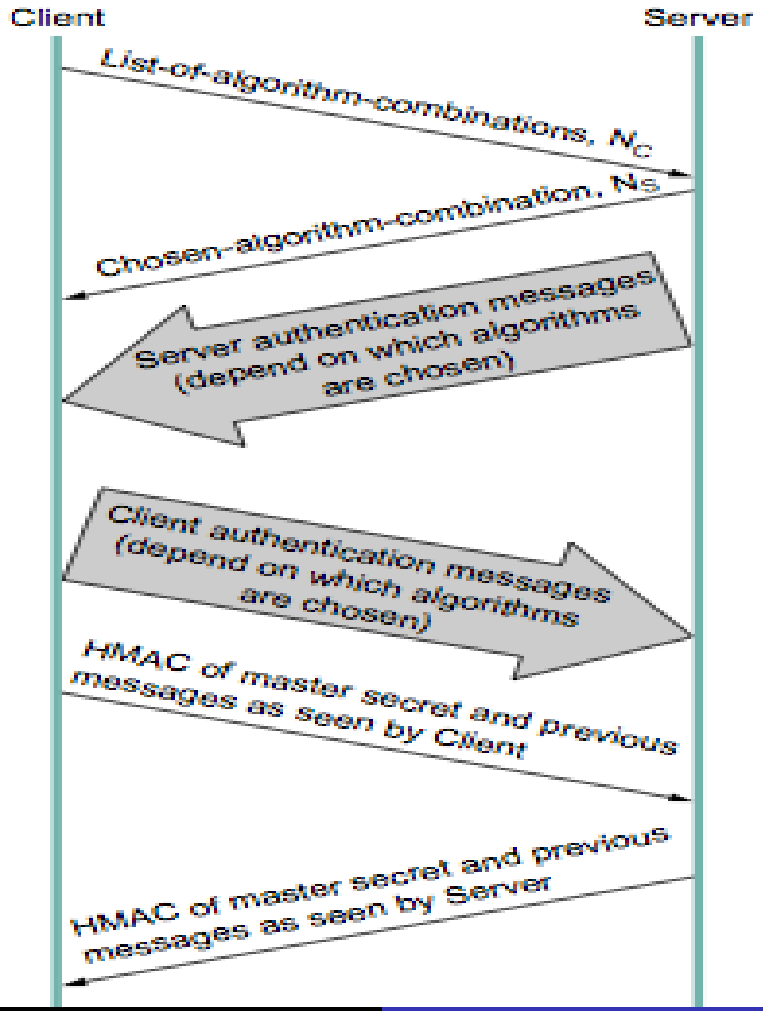
Handshake SSL

- Se **negocian** los **algoritmos** a utilizar durante la conexión.
- Se **autentica** al servidor o los dos entes.
- Se genera un canal seguro para definir una **master key**.
- Se derivan las **claves** necesarias a partir de la master.
- Se constata la **integridad** de todos los mensajes de intercambio de claves.

Ejercicio 5

- ¿Qué información tienen disponible ambos extremos antes de iniciar el handshake?
- Describa una posible implementación de un handshake para establecer una conexión segura.

A alto nivel


Client
Server
List-of-algorithm-combinations, N_C
Chosen-algorithm-combination, N_S
Server authentication messages (depend on which algorithms are chosen)
Client authentication messages (depend on which algorithms are chosen)
HMAC of master secret and previous messages as seen by Client
HMAC of master secret and previous messages as seen by Server

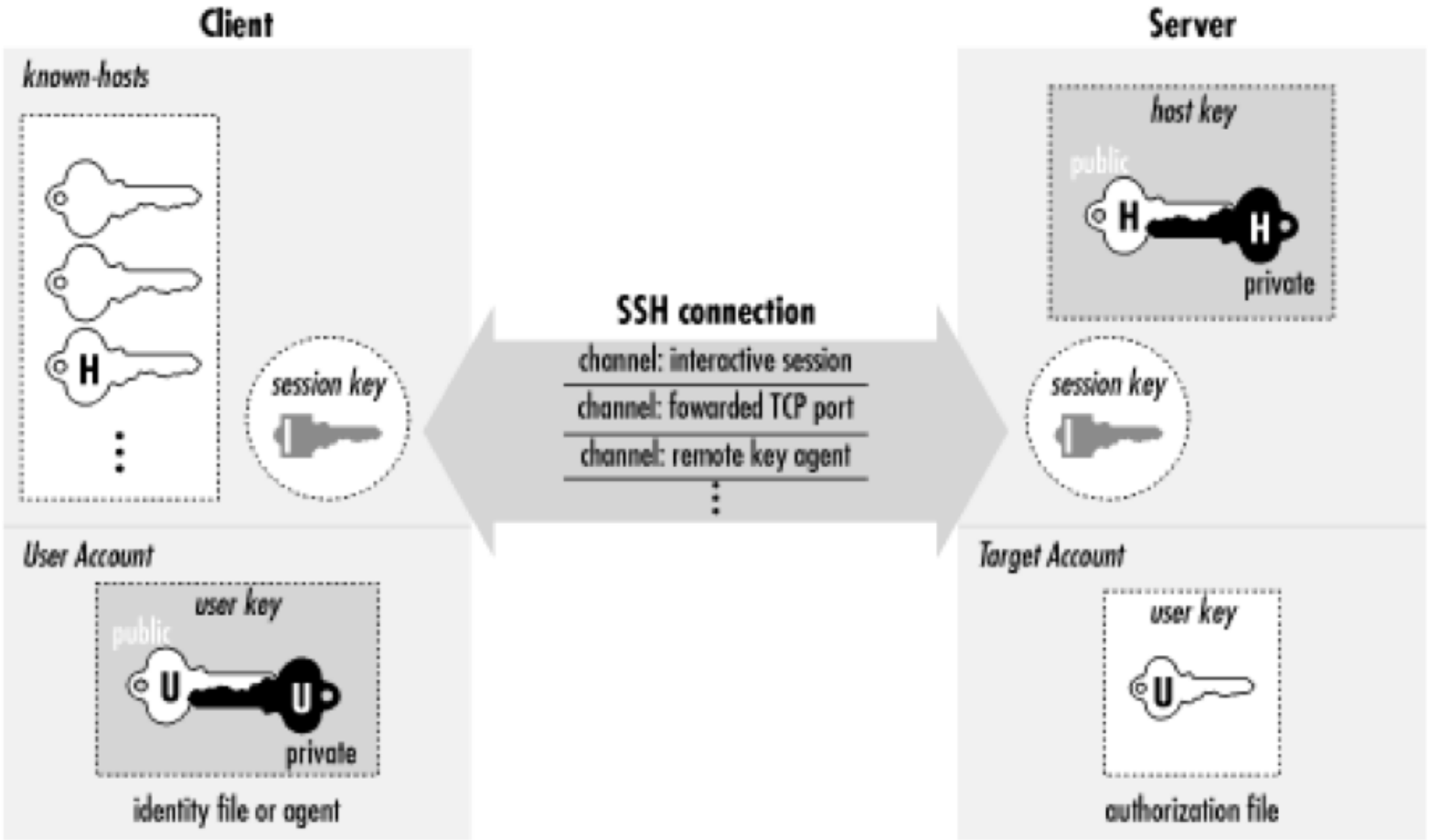
SSH

Es un protocolo para acceder a máquinas remotas de manera segura

- Alternativa segura a Telnet y Ftp.
- Provee autenticación, confidencialidad y integridad.
- Permite hacer cosas más avanzadas como redirigir la salida de aplicaciones a través de canales seguros (port fowarding).
- Ese es un caso particular de túneles seguros.

Las fases SSH son similares a las fases TLS.

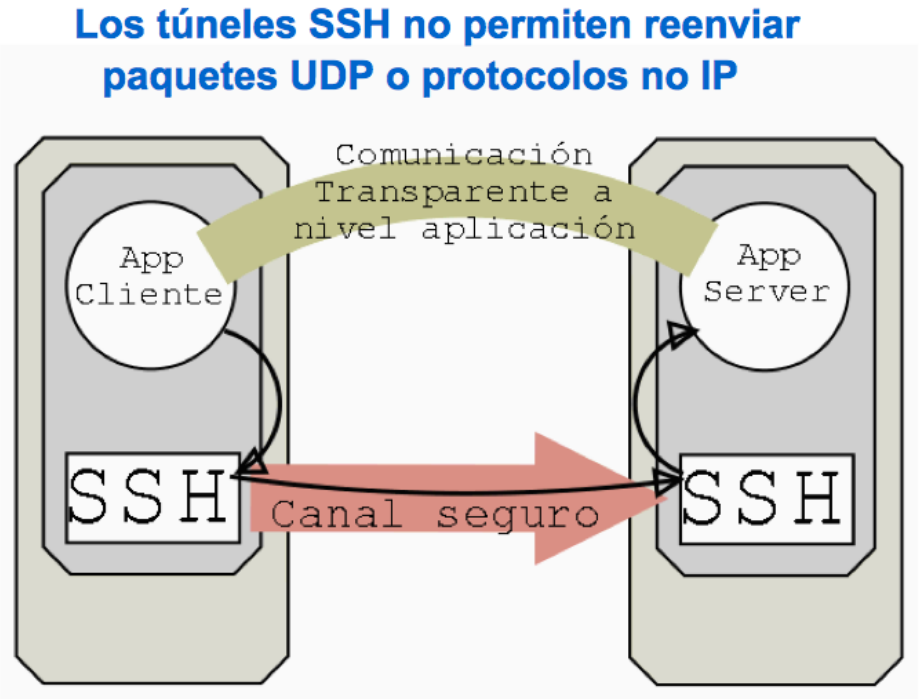
Handshake SSH a alto nivel



Túnel SSH

Sirven para:

- proteger claves de protocolos inseguros (Ftp, Telnes, IMAP).
- Atravesar Firewalls (si permiten ssh).
- Acceder a servicios internos de una LAN con ip privadas.



Seguridad en correos electrónicos

Dos esquemas:

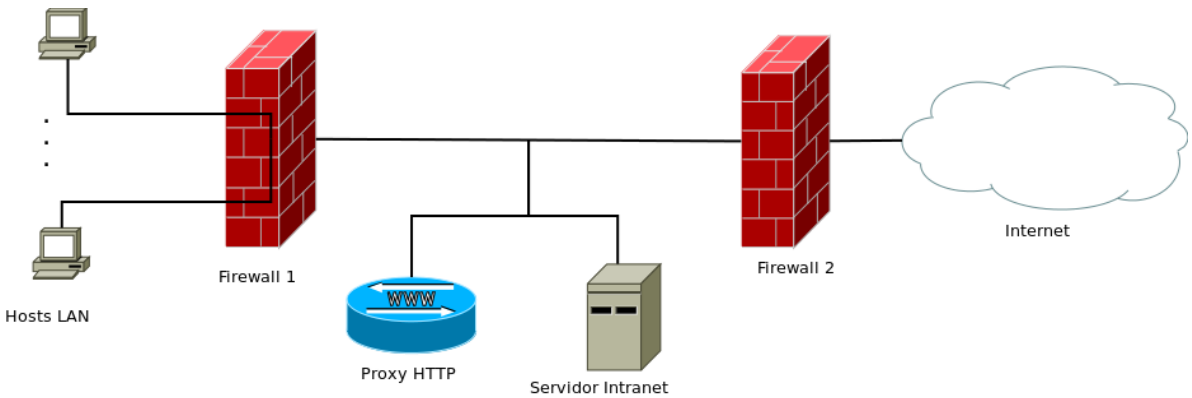
PGP

- Confidencialidad y autenticación.
- La gestión de claves se basa en un esquema de confianza.

S/Mime

- Certificados X509 y PKI.
- Confidencialidad y autenticación.

La empresa Sinegociamostegarco diseñó un nuevo esquema de seguridad para la red interna colocando los servicios accedidos desde internet en una DMZ. Ésta cuenta con el servicio de intranet (sobre HTTP) para que los empleados carguen las horas y tareas en las que fueran esclavizados cada mes y un Proxy HTTP para resolver los recursos HTTP provenientes de la intranet.



Establecer un criptosistema para garantizar la autenticidad del Proxy y del servidor de la intranet. Enumere los elementos utilizados y explique cómo esta solución impide ataques de *Man in the middle*.

¿Repasando...?

¿Dudas?,

¿Preguntas?